

AMENDMENTS TO THE CLAIMS

1. (Currently amended) A method for virtualizing access to native resources, the method comprising the steps of:

(a) receiving a request to access a native resource from a process executing within a in the context of an isolation environment including an application isolation layer and a user isolation layer, the request including a virtual name for the native resource;

(b) determining that a rule action of remap is associated with the virtual name included in the received request;

(c) forming a literal name for the native resource, the literal name identifying a literal native resource of the same type as the requested resource; and

(d) issuing to the operating system a request to access the native resource, the request including the determined literal name for the native resource.

2. (Original) The method of claim 1 wherein step (a) comprises receiving a request from a process executing in the context of an isolation environment to access a named system object, the request including a virtual name for the system object.

3. (Original) The method of claim 2 wherein step (c) comprises:

(c-1) determining a rule associated with the virtual name included in the received request; and

(c-2) using the determined rule to form a literal name for the system object that identifies a literal system object.

4. (Original) The method of claim 1 wherein step (a) comprises receiving a request from a process executing in the context of an isolation environment to access a file system element, the request including a virtual name for the file system element.

5. (Original) The method of claim 4 wherein step (c) comprises:

(c-1) determining a rule associated with the virtual name included in the received request; and

(c-2) using the determined rule to form a literal name for the file system element that identifies a literal file system element.

6. (Original) The method of claim 1 wherein step (a) comprises receiving a request from a process executing in the context of an isolation environment to access a registry key, the request including a virtual name for the registry key.

7. (Original) The method of claim 6 wherein step (c) comprises:

(c-1) determining a rule associated with the virtual name included in the received request; and

(c-2) using the determined rule to form a literal name for the registry key that identifies a literal registry key.

8. (Original) The method of claim 1 wherein step (a) comprises receiving a request from a process executing in the context of an isolation environment to access one of a window and a window class, the request including one of a virtual name for the window and a virtual name for the window class.

9. (Original) The method of claim 8 wherein step (c) comprises:

(c-1) determining a rule associated with the virtual name included in the received request; and

(c-2) using the determined rule to form a literal name for the one of a virtual name for the window and a virtual name for the window class that identifies one of a literal window name and a literal window class.

10. (Original) The method of claim 1 wherein step (c) comprises:

(c-1) accessing a rules engine to determine a rule associated with the virtual name received in the request; and

(c-2) forming a literal name for the native resource responsive to the determined rule, the formed literal name identifying a literal native resource of the same type as the requested

resource.

11. (Original) The method of claim 1 further comprising the step of receiving a handle from the operating system identifying the accessed object.

12. (Original) The method of claim 11 further comprising the step of transmitting the handle to the process.

13. (Original) The method of claim 1 wherein step (c) further comprises determining, by the remap rule, the literal name of the native resource for the virtual name of the native resource.

14. (Currently amended) A ~~computer-implemented~~ apparatus provided by an operating system executing on a processor of a computer and for virtualizing access to native resources, the apparatus comprising:

a hooking mechanism receiving a request to access a native resource from a process executing in the context of an isolation environment including an application isolation layer and a user isolation layer, the request including a virtual name for the native resource;

a name virtualization engine forming a literal name for the native resource, the formed literal name identifying a literal native resource of the same type as the requested resource; and
an ~~operating system~~ interface of an operating system executing on a processor of a computer, the interface requesting access to the identified literal native resource.

15. (Original) The apparatus of claim 14 wherein the hooking mechanism intercepts a request to open a native resource.

16. (Original) The apparatus of claim 14 wherein the hooking mechanism intercepts a request to create a native resource.

17. (Original) The apparatus of claim 14 further comprising a rules engine storing a rule associated with the virtual name included in the received request.

18. (Original) The apparatus of claim 17 wherein the rules engine comprises a database.
19. (Original) The apparatus of claim 17 wherein the rule engine comprises a rule to determine the literal name of the native resource from the virtual name of the native resource.
20. (Original) The apparatus of claim 14 wherein the hooking mechanism comprises a file system filter driver.
21. (Original) The apparatus of claim 14 wherein the hooking mechanism comprises a mini-filter.
22. (Original) The apparatus of claim 14 wherein a native file system comprises the hooking mechanism.